Progress on the Federal S/MIME V3 Client Profile

Michael Chernick

chernick@nist.gov

+1-301-975-3610

November 8, 2001

1901-2001

NIST CENTENNIAL

NIST S/MIME Group

Mission: To accelerate deployment of secure interoperable S/MIME Products

Major Projects:

- In-house Laboratory
- S/MIME V3 Client Profile
- Internet-based S/MIME Test Facility

NIST S/MIME CLIENT Profile (Purpose)

- To Identify Subset of S/MIME V3 Specifications That:
  - –Helps to Assure Interoperability
  - –Promotes Secure Communications at Reasonable Cost
  - –Serves as Basis for Test Development
- As Guidance for COTS Product Procurement and Development

S/MIME Profile Requirements (1)

- Mandatory Parts of RFCs 2630, 2632, and 2633
  - Except Diffie-Hellman Key Agreement not required
- Mandatory Algorithm Suites, plus…
  - Requires support for both RSA (V1.5, RFC2313) and DSA (FIPS186-2) digital signatures
  - Key Size at least 1024 bits for RSA and DSA
  - D-H Keys and Derivation of KEKs as Defined in RFC 2631 is *encouraged* but NOT required

S/MIME Profile Requirements (2)

- Selected Features Required From RFC 2634, Enhanced Security Services
  - Signed Receipts
    - Request (Non-Third Party) Signed Return Receipt
    - Generate Signed Return Receipt Upon Request
    - Match Signed Receipt to Original Message
  - Mail List Client Processing
    - mlExpansionHistory attribute MUST be processed

S/MIME Profile Requirements (3)

- Message Generation Requirements
  - Send “Clear” Signed Messages
    - Must Be Able to Generate/Include SignerInfo, SMIMECapabilities Attribute, User Certs and CRLs
  - Send Encrypted and Both Signed & Encrypted Messages
  - Send to Multiple Recipients
- Message Reception Requirements
  - Receive Both “Clear” and “Opaque”
  - Receive and Decrypt Messages Sent to Multiple Recipients

Certificate Processing

- PKIX (RFC 2459) & U.S. Federal X.509 Cert/CRL Extensions Profile
  - Implementations Must Be Able to Construct Cert. Paths Between Accepted Trust Points and Sender’s or Recipient's Certs.
    - Tests will include paths with multiple CA certificates
    - Testing will require use of LDAP and processing standard directory attributes (See RFC 2587)
  - Must Be Able to Perform Path Validation According to RFC 2459, Section 6.

NIST S/MIME CLIENT Profile (Status)

- Public Comments Received
  - Comment Period Ended on 17 September
  - Most ask for clarifications/better wording
  - One asks for removal of signed receipt processing mandate

- Updated Document Available Mid November
  - http://csrc.ncsl.nist.gov/pki/smime/draft_SMIMEProfile.pdf

- Executive Summary Added
  - For Procurement Officials, Implementers, Vendors, etc.
  - Background information on email and S/MIME
  - Summary of Mandatory and Optional Features
  - Available Mid November at http://csrc.ncsl.nist.gov/pki/smime

NIST S/MIME CLIENT Profile Major Comment

•One Major Comment Received from Entrust (7 Aug 2001)

- Asks for removal of signed receipt processing mandate
- "Clause 3.1 requires support for signed receipts, an enhanced security service that is optional in the base S/MIME standard. Signing S/MIME messages can frequently be used to support provision of security services that do not require signed receipts, such as ensuring the integrity of the message content. The signed receipts service supports additional security services such as proof of delivery and some support for non-repudiation. These additional security services are not required for the vast majority of signed messages and in many environments they cannot be sent anyway because auto response features are turned off in the clients. Adding support for signed receipts to S/MIME client systems is a significant undertaking that adds complexity as well as cost to S/MIME client systems. Because this service will only be required for a subset of secured messaging, support for this service should be optional in the Federal S/MIME V3 Client profile. This would allow the cost of this additional functionality to be bourne by the agencies that require this service, enabling other agencies that do not require the service to obtain less complex and less costly S/MIME v3 client systems. Agencies that do not want/need signed receipts should not be required to request it in their purchases of messaging systems."
- Sharon Boeyen, Entrust, Principal, Advanced Security

NIST S/MIME CLIENT Profile Major Comment (Continued)

- One Major Comment Received from Entrust
  - Asks for removal of signed receipt processing mandate
  - NIST feels that signed receipt processing is important for Federal Agencies and NIST believes that mandating signed receipt processing will ultimately make for better S/MIME products at, perhaps, slightly higher prices, but with ubiquitous support for signed receipt processing.
  - NIST asks for comments on this mandate from Federal Agencies
  - One Agency asked says “Yes, mandate signed receipts”

NIST S/MIME CLIENT Profile Major Comment (Continued)

- NIST Solicits Further Comments on Issue of Mandating Signed Receipt Processing
- Comments from anybody considered but emphasis is on comments from users especially from Federal Agencies
- Comment period ends 30 November
- Comments to Mike Chernick (chernick@nist.gov)

Automated S/MIME Test Facility

- Developing Internet-based Automated Testing Facility
  - Using Getronics S/MIME Freeware Library (SFL) as Reference Implementation
  - Test Scenarios Intended to Cover Profile Requirements and Options (But NOT Out-of-Scope S/MIME Features)
- Ensure Conformance of Vendor Implementations to S/MIME V3 Client Profile
  - Web Based Info. & Instructions, But Will Use SMTP for Testing
  - Support for Both Originator and Recipient Roles (Will Require "Human Scoring" & Self-Scoring for Some Tests)
- Also, Identify Ambiguities & Errors in IETF Specifications, NIST Profile, and SFL reference code

Goals/Notes for Automated Test Facility

- Objective Testing Wherever Possible
- Anonymous Testing Possible
- Results Only to Remote Tester
- All Required Communications thru Email
- Not Publishing Remote Tester's Certs/CRLs
- Using Test Policy OIDs

Status of Automated Test Facility

- Early Release of Software Received
- Expect Release for “Beta” Testing in December
- Limited Test Cases at First (Others phased in later)
- A Few Beta Testers Identified
- Targeting Public Availability in Q1 of 2002
- Additional Test Cases To Be Added through 2002

More Information

- **NIST S/MIME Page**

  http://csrc.nist.gov/pki/smime

- **S/MIME Draft Profile Page**

  http://csrc.ncsl.nist.gov/pki/smime/draft_SMIMEProfile.pdf

- **Point of Contact**
  - **Michael Chernick** **chernick@nist.gov**
    +1 301-975-3610